

#2

PATENT  
81942.0014

Express Mail Label No. EL 713 695 977 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Masao KASAHARA

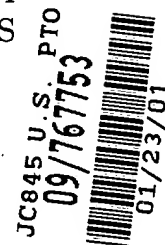
Serial No: Not assigned

Filed: January 23, 2001

For: ENCRYPTION METHOD, DECRYPTION  
METHOD, CRYPTOGRAPHIC  
COMMUNICATION METHOD AND  
CRYPTOGRAPHIC COMMUNICATION  
SYSTEM

Art Unit: Not assigned

Examiner: Not assigned



TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION  
Assistant Commissioner for Patents  
Washington, D.C. 20231

Dear Sir:

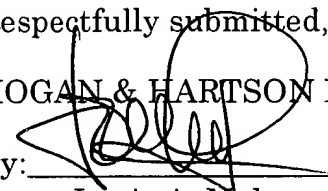
Enclosed herewith are certified copies of Japanese patent application Nos. 2000-016357 filed January 25, 2000 and 2000-073033 filed March 15, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: January 23, 2001

By:   
Louis A. Mok  
Registration No. 22,585  
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900  
Los Angeles, California 90071  
Telephone: 213-337-6700  
Facsimile: 213-337-6701

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application:

2000年 3月15日

出 願 番 号  
Application Number:

特願2000-073033

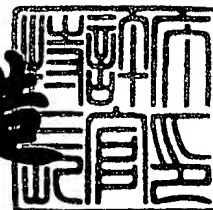
出 願 人  
Applicant(s):

村田機械株式会社  
笠原 正雄

2000年 8月18日

特許庁長官  
Commissioner,  
Patent Office

及 川 耕 造



出証番号 出証特2000-3064846

【書類名】 特許願

【整理番号】 21058

【提出日】 平成12年 3月15日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00  
H04L 9/00

【発明の名称】 暗号化方法

【請求項の数】 3

【発明者】

    【住所又は居所】 大阪府箕面市粟生外院4丁目15番3号

    【氏名】 笠原 正雄

【特許出願人】

    【識別番号】 000006297

    【氏名又は名称】 村田機械株式会社

    【代表者】 村田 純一

【特許出願人】

    【識別番号】 597008636

    【氏名又は名称】 笠原 正雄

【復代理人】

    【識別番号】 100114557

    【弁理士】

    【氏名又は名称】 河野 英仁

    【電話番号】 06-6944-4141

【代理人】

    【識別番号】 100078868

    【弁理士】

    【氏名又は名称】 河野 登夫

    【電話番号】 06-6944-4141

【先の出願に基づく優先権主張】

【出願番号】 特願2000- 16357

【出願日】 平成12年 1月25日

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化方法

【特許請求の範囲】

【請求項 1】 暗号化すべき平文を分割した分割平文と公開鍵とを用いて積和型の暗号文を作成する暗号化方法において、前記積和型の暗号文を有限体上で構成することを特徴とする暗号化方法。

【請求項 2】 前記分割平文を符号化し、中間復号文の各項を誤り訂正符号語で構成する請求項 1 記載の暗号化方法。

【請求項 3】 前記分割平文毎に複数の公開鍵を予め準備しておき、各分割平文について前記複数の公開鍵から任意の公開鍵を選択し、選択した公開鍵を使用して暗号文を作成する請求項 1 または 2 記載の暗号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、公開鍵を用いて平文を暗号文に変換する公開鍵暗号系の暗号化方法に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュタリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換するこ

とである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

## 【0004】

暗号化方式は、大別すると共通鍵暗号系と公開鍵暗号系との二つに分類できる。共通鍵暗号系では、暗号化鍵と復号鍵とが等しく、送信者と受信者とが同じ共通鍵を持つことによって暗号通信を行う。送信者が平文を秘密の共通鍵に基づいて暗号化して受信者に送り、受信者はこの共通鍵を用いて暗号文を元に平文に復号する。

## 【0005】

これに対して公開鍵暗号系では、暗号化鍵と復号鍵とが異なっており、公開されている受信者の公開鍵で送信者が平文を暗号化し、受信者が自身の秘密鍵でその暗号文を復号することによって暗号通信を行う。公開鍵は暗号化のための鍵、秘密鍵は公開鍵によって変換された暗号文を復号するための鍵であり、公開鍵によって変換された暗号文は秘密鍵でのみ復号することができる。

## 【0006】

公開鍵暗号系の1つの方式として、積和型暗号方式が知られている。これは、送信者である一方のエンティティ側で平文をK分割した平文ベクトル  $m = (m_1, m_2, \dots, m_K)$  と公開鍵である基数ベクトル  $c = (c_1, c_2, \dots, c_K)$  とを用いて、暗号文  $C = m_1 c_1 + m_2 c_2 + \dots + m_K c_K$  を作成し、受信者である他方のエンティティ側でその暗号文Cを秘密鍵を用いて平文ベクトルmに復号して元の平文を得る暗号化形式である。従来の積和型暗号方式では、整数環上の演算を利用している。

## 【0007】

【発明が解決しようとする課題】

このような積和型暗号に関して、安全性の向上、処理時間の高速化等の観点に基づいて種々の新規の暗号方式が提案、研究されている。

## 【 0 0 0 8 】

元来、このような積和型暗号は、公開されている基数ベクトル  $c$  の各成分から平文ベクトル  $m$  の各成分を解読する数学的な  $LLL$  (Lenstra-Lenstra-Lovasz) 法による攻撃を受け易いという特徴を持っており、この  $LLL$  法に対して強い積和型暗号化方法の開発が望まれている。

## 【 0 0 0 9 】

本発明は斯かる事情に鑑みてなされたものであり、有限体上で暗号系を構成することにより、 $LLL$  法による攻撃に対して強く、安全性を向上できる新しい手法の積和型の暗号化方法を提供することを目的とする。

## 【 0 0 1 0 】

## 【課題を解決するための手段】

請求項 1 に係る暗号化方法は、暗号化すべき平文を分割した分割平文と公開鍵とを用いて積和型の暗号文を作成する暗号化方法において、前記積和型の暗号文を有限体上で構成することを特徴とする。

## 【 0 0 1 1 】

請求項 2 に係る暗号化方法は、請求項 1 において、前記分割平文を符号化し、中間復号文の各項を誤り訂正符号語で構成することを特徴とする。

## 【 0 0 1 2 】

請求項 3 に係る暗号化方法は、請求項 1 または 2 において、前記分割平文毎に複数の公開鍵を予め準備しておき、各分割平文について前記複数の公開鍵から任意の公開鍵を選択し、選択した公開鍵を使用して暗号文を作成することを特徴とする。

## 【 0 0 1 3 】

第 1 発明では、秘密鍵、公開鍵、乱数等を多項式表現して、整数環上ではなく有限体上で積和型暗号系を構成する。よって、整数環上での積和型暗号系に比べて  $LLL$  法による攻撃に対して強く、安全性が向上する。

## 【 0 0 1 4 】

第2発明では、中間復号文の各項が誤り訂正符号語で構成されるようになっており、多少の誤りが発生しても、その符号語の訂正能力により元の平文を正確に復号できる。

## 【0015】

第3発明では、平文を分割した分割平文毎に複数の公開鍵が予め準備されており、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文毎に選択し、選択した公開鍵を使用して暗号文を作成する。よって、公開鍵を選択できるので、つまり、送信者であるエンティティ側で自由に公開鍵を選択して暗号文を作成できるので、その公開鍵の選択の仕方が攻撃者には不明であるため、攻撃は困難となり、安全性が高い。

## 【0016】

## 【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

まず、本発明における多項式表現について説明する。後述する第1実施の形態におけるクラス選択情報、または、後述する第2実施の形態における誤り訂正検出のために平文Mが符号化されたメッセージmを下記(1)とする。なお、Kは平文Mの分割数を示す。

$$m = (m_1, m_2, \dots, m_K) \quad \dots (1)$$

なお、メッセージmの各成分 $m_i$  ( $i = 1, 2, \dots, K$ )は有限体(ガロア体) $F_q$ 上の $k_i$ 次元のベクトルであるが、ここでは説明を簡単にするために、 $q = 2$ 、且つ、 $k_i = k$  (一定)とする。

## 【0017】

このように、メッセージmは予め符号化されているので、このことを強調したい場合にはメッセージmの成分 $m_i$ を $m_i'$ として、その $m_i'$ を下記(2)のように表す。但し、 $m_{ij}' \in F_2$ である。また、その成分 $m_i$ を多項式表記では、下記(3)のように表す。

## 【0018】



【数 1】

$$m_i' = (m_{i1}', m_{i2}', \dots, m_{ik}') \quad \dots (2)$$

$$m_i'(X) = m_{i1}' + m_{i2}'X + \dots + m_{ik}'X^{k-1} \quad \dots (3)$$

【0019】

なお、本明細書ではある値Aをベクトルsまたは多項式s(X)と表すが、このベクトルs, s(X)を夫々Aのベクトル表現, 多項式表現と呼ぶ。

【0020】

(第1実施の形態：有限体上での積和型暗号で公開鍵を任意選択)

図1は、第1実施の形態による暗号化方法・復号方法をエンティティa, b間の情報通信に利用した状態を示す模式図である。図1の例では、一方のエンティティa側で、平文Mを暗号文Cに暗号化し、通信路1を介してその暗号文Cを他方のエンティティbへ送信し、エンティティb側で、その暗号文Cを元の平文Mに復号する場合を示している。

【0021】

送信側であるエンティティaには、平文Mを複数の分割平文に分割する平文分割器2と、各分割平文に対する公開鍵をデータベース10から選択する公開鍵選択器5と、選択した公開鍵と各分割平文とを用いて暗号文Cを作成する暗号化器3とが備えられている。また、受信側であるエンティティbには、送られてきた暗号文Cを元の平文Mに復号する復号器4が備えられている。第1実施の形態では、後述するように、秘密鍵, 公開鍵, 乱数等を多項式表現して、有限体上で積和型暗号系を構成する。

【0022】

[第1実施の形態の第1例]

図2は、各分割平文毎に複数の公開鍵を予め格納しているデータベース10内の公開鍵リスト(基数リスト)を示す図である。図2において、Kは平文Mの分割数(クラス数)、Jは各クラスi(i=2, 3, ..., K)における選択対象

の公開鍵（基数）の総数を表す。クラス 1 を除いて、各分割平文毎（各クラス毎）に J 組の公開鍵（基数）が準備されている。

【0023】

そして、送信者であるエンティティ a 側では、このような公開鍵（基数）を格納しているデータベース 10 から、各分割平文毎（各クラス毎）に 1 組ずつの公開鍵（基数）を任意に選択して読み出し、読み出した K 組の公開鍵（基数）を暗号化鍵として利用する。ここで、エンティティ a に許される公開鍵（基数）の可能な選択組合せは  $J^{K-1}$  通りである。この  $J^{K-1}$  通りの公開鍵（基数）の組合せが存在することに、有限体上での構成に加えた第 1 実施の形態での更なる安全性の基盤がある。

【0024】

（準備）

各記号を以下のように定義する。

$m_i$  : メッセージ m の成分  $m_i \in F_q$  ( $q = 2^k$ )

$\alpha_i, \beta_i$  : 乱数  $\alpha_i, \beta_i \in F_q$

$v_i$  : 公開鍵リストのクラス i に所属する  $F_q$  上の乱数ベクトル

$b_i$  : 基数  $b_i = \alpha_i + \beta_i X$

【0025】

（暗号化）

秘密鍵と公開鍵とを以下のように準備する。

・秘密鍵：  $\{b_i(X)\}, \{v_i(X)\}, w(X), P(X),$

置換行列  $P(*)$

・公開鍵：  $\{c_i^{(j)}(X)\}, F_q$

【0026】

$P(X)$  を適切に選ばれた秘密の既約多項式として、下記（4）を導く。

【0027】

【数2】

$$b_1(X)b_2(X)\cdots b_i(X)v_{i+1}^{(j)}(X)w(X) \\ \equiv c_i^{(j)}(X) \pmod{P(X)} \quad \cdots (4)$$

【0028】

なお、図2には選択対称の複数の公開鍵を多項式表現  $b_1(X) b_2(X) \cdots b_{i-1}(X) v_i(X)$  で示しているが、これはベクトル表現  $b_1 b_2 \cdots b_{i-1} v_i$  に対応する。

【0029】

暗号化を、 $F_q$  上で下記(5)のように行う。

【0030】

【数3】

$$C(X) = \sum_{i=1}^K m_i' c_i^{(j)}(X) \quad \cdots (5)$$

【0031】

(復号)

下記(6)を満たす秘密の多項式  $w^{-1}(X)$  を用いて、中間復号文  $M(X)$  を  $M(X) \equiv C(X) w^{-1}(X) \pmod{P(X)}$  として、下記(7)のように導く。但し、 $1 \leq j \leq J$  である。

$$w(X) w^{-1}(X) \equiv 1 \pmod{P(X)} \quad \cdots (6)$$

【0032】

【数4】

$$\begin{aligned} C(X)w^{-1}(X) \\ \equiv m_1'v_1(X) + m_2'b_1(X)v_2^{(j)}(X) + \dots \\ + m_K'b_1(X)b_2(X)\dots b_{K-1}(X)v_K^{(j)}(X) \pmod{P(X)} \\ \dots (7) \end{aligned}$$

【0033】

中間復号文 $M(X)$ の最下位項の $m_1'v_1(X)$ を復号した後は、第2項以降を同様に復号できる。

【0034】

$b_1(X)$ を法とする $v_1(X)$ の逆元 $v_1^{-1}(X)$ を用いて、下記(8)を導く。ここで、図2に示すように、クラス1にあっては基数( $v_1(X)$ )が一義的に選択される。

【0035】

【数5】

$$M(X)v_1(X)v_1^{-1}(X) \equiv m_1' \pmod{b_1(X)} \dots (8)$$

【0036】

$m_1'$ より元の平文の符号化された成分 $m_1$ を復号すると共に、下記(9)に従って、クラス2における基数(公開鍵)の選択情報を復号する。

$$m_1' \equiv j \pmod{J} \dots (9)$$

【0037】

これによって、クラス2において選択された基数(公開鍵 $b_1(X)v_2^{(j)}(X)$ )が特定されるので、 $m_1'$ と全く同様にして $m_2'$ を復号することができる。即ち、下記(10)に従って、 $m_2'$ を復号する。以下同様の処理により、 $m_3' \sim m_K'$ を復号する。

【0038】

【数 6】

$$\begin{aligned}
& \frac{M(X) - m_1' v_1(X)}{b_1(X)} \\
&= m_2' v_2^{(1)}(X) + m_3' b_2(X) v_3^{(1)}(X) \\
&+ \dots + m_K' b_2(X) \dots b_{K-1}(X) v_K^{(1)}(X) \quad \dots (10)
\end{aligned}$$

【0039】

以上のように、第1例では、積和型暗号文に対して、最下位項のメッセージを最初に復号し、その後、上位項側のメッセージを順次的に復号する場合について説明したが、これとは逆に、最上位項のメッセージを最初に復号した後、下位項側のメッセージを順次的に復号するようにしても良い。

【0040】

〔第1実施の形態の第2例〕

図3は、各分割平文毎に複数の公開鍵を予め格納しているデータベース10内の公開鍵リスト（基数リスト）を示す図である。図3において、Kは平文Mの分割数（クラス数）、Jは各クラスi（i=1, 2, ..., K-2）における選択対象の公開鍵（基数）の総数を表す。K-1番目、K番目を除く各分割平文毎（各クラス毎）にJ個の公開鍵（基数）が準備されている。

【0041】

そして、送信者であるエンティティa側では、このような公開鍵（基数）を格納しているデータベース10から、各分割平文毎（各クラス毎）に1組ずつの公開鍵（基数）を任意に選択して読み出し、読み出したK組の公開鍵（基数）を暗号化鍵として利用する。ここで、エンティティaに許される公開鍵（基数）の可能な選択組合せは $J^{K-2}$ 通りである。

【0042】

（準備）

各記号を以下のように定義する。

$m_i'$  : メッセージmの成分  $m_i' \in F_q$  ( $q = 2^k$ )

$\alpha_i^{(j)}, \beta_i^{(j)}$  : 乱数  $\alpha_i^{(j)}, \beta_i^{(j)} \in F_q$   
 $b_i$  : 基数  $b_i^{(j)}(X) = \alpha_i^{(j)} + \beta_i^{(j)} X$

【0043】

(暗号化)

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵:  $\{b_i(X)\}, w(X), P(X),$  置換行列  $P(*)$
- ・公開鍵:  $\{c_i^{(j)}(X)\}, F_q$

【0044】

$P(X)$  を適切に選ばれた秘密の多項式として、下記 (11) を導く。

【0045】

【数 7】

$$b_i^{(j)}(X)w(X) \equiv c_i^{(j)}(X) \pmod{P(X)} \cdots (11)$$

【0046】

ここで、ベクトル  $c_i^{(j)}$  の成分は秘密の置換行列  $P(*)$  によってランダムに配置される。図 3 には、 $b_i^{(j)}(X)$  のベクトル表現を  $b_i^{(j)}$  として示している。前述したように、図 3 のクラス  $K-1, K$  において唯一つの基数しか使われていないが、これは後述するように高速復号を可能にするためである。

【0047】

暗号化を、 $F_q$  上で下記 (12) のように行う。

【0048】

【数 8】

$$C(X) = \sum_{i=1}^K m_i' c_i^{(j)}(X) \cdots (12)$$

【0049】

(復号)

下記 (13) を満たす秘密の多項式  $w^{-1}(X)$  を用いて、中間復号文  $M(X)$  を

$M(X) \equiv C(X) w^{-1}(X) \pmod{P(X)}$  として、下記 (14) のように導く。但し、 $1 \leq j \leq J$  である。

$$w(X) w^{-1}(X) \equiv 1 \pmod{P(X)} \quad \dots (13)$$

【0050】

【数9】

$$\begin{aligned} C(X)w^{-1}(X) \\ \equiv m_1' b_1^{(j)}(X) + m_2' b_2^{(j)}(X) + \dots \\ + m_K' b_K(X) \pmod{P(X)} \dots (14) \end{aligned}$$

【0051】

中間復号文  $M(X)$  の最上位項の  $m_K'$  を復号すれば、上位第2項  $m_{K-1}'$  から最下位項  $m_1'$  までは同様に復号できるので、ここでは  $m_K'$  の復号を中心に以下に説明する。

【0052】

一般にベクトル  $M$  の基数  $b_{i-1}^{(j)}$ ,  $b_i^{(j)}$  に関連する  $2k$  桁をサンプルする操作を  $S^i(M)$  とし、サンプルされた系列を多項式で  $S_M^i(X)$  と表記する。式 (14) で与えられる中間復号文  $M(X)$  に対し、最上位  $2k$  桁をサンプルした系列  $S_M^K(X)$  は下記 (15) で与えられる。但し、 $e_{K-1}(X)$  は上位第2項  $m_{K-1}'(X) b_{K-1}(X)$  の上位  $k$  桁の多項式表現である。

【0053】

【数10】

$$S_M^K(X) = m_K'(X) b_K(X) + e_{K-1}(X) \dots (15)$$

【0054】

上記  $e_{K-1}(X)$  を一般にポストフィックスと呼ぶ。下記 (16) に従って  $e_{K-1}(X)$  を導き、下記 (17) に従ってメッセージ  $m_K'(X)$  を復号することができる。

【0055】

【数11】

$$S_M^K(X) \equiv e_{K-1}(X) \pmod{b_K(X)} \cdots (16)$$

$$\frac{S_M^K(X) - e_{K-1}(X)}{b_K(X)} = m_K'(X) \cdots (17)$$

【0056】

ここで、図3に示したように、クラス $K-1$ 、 $K$ においては選択の余地がなく、夫々のクラスにおいて $b_{K-1}$ 、 $b_K$ が一意的に選ばれている。 $m_K'$ より原情報 $m_K$ を復号すると共に、下記(18)に従って、クラス $K-2$ における基数の選択情報を復号する。より一般的には、 $m_i' \equiv j \pmod{J}$ により、クラス $i-2$ における基数選択情報を得る。

$$m_K' \equiv j \pmod{J} \quad \cdots (18)$$

【0057】

このように2つあとのクラスの基数選択情報を復号するのは、クラス $i-2$ に対応して与えられる $S_M^{i-2}(M)$ の復号に入る前に基数 $b_{i-2}^{(j)}$ を準備しておくためである。このことにより、復号プロセスを遅滞させることなく逐次的に実行することができる。

【0058】

$m_K' \equiv j \pmod{J}$ によって、クラス $K-2$ における基数 $b_{K-2}^{(j)}$ の形が特定されるので、 $m_K'$ と全く同様にして $m_{K-2}'$ を復号することができる。なお、 $m_{K-1}'$ は下記(19)のようにあらためておくことにより、 $m_K'$ と全く同様にして復号することができる。以下、同様のプロセスで $m_1' \sim m_{K-2}'$ を、高次側メッセージより順次復号することができる。

【0059】



【数12】

$$M^{K-1}(X) = M^K(X) + m_K'(X) b_K(X) X^{K-1} \dots (19)$$

【0060】

上述した第1例では、メッセージの復号処理と基数の選択情報の復号処理とを並列的に行うことはできないが、第2例では、 $i$  番目のメッセージの復号時にクラス  $i-2$  における基数の選択情報を得ることができるので、メッセージの復号処理と基数の選択情報の復号処理とを、具体的には  $i$  番目における上記(16)の演算と  $i-1$  番目における上記(17)の演算とを並列的に行え、所謂パイプライン処理が可能となって、第2例では、第1例に比べて、復号処理の更なる高速化を図れる。

【0061】

なお、上記第2例では、積和型暗号文に対して、最上位項のメッセージを最初に復号し、その後、下位項側のメッセージを順次的に復号するようにしたが、これとは逆に、最下位項のメッセージを最初に復号した後、上位項側のメッセージを順次的に復号するようにしても良い。

【0062】

次に、以上のような第1実施の形態における安全性について説明する。クラス  $i$  における  $j$  番目の公開鍵  $c_i^{(j)}(X)$  を、下記(20)のように表す。

【0063】

【数13】

$$c_i^{(j)}(X) = c_{i1}^{(j)} + c_{i2}^{(j)} + \dots + c_{iK}^{(j)} X^{K-1} \dots (20)$$

【0064】

クラス  $i$  におけるメッセージ  $m_i$  が  $F_q$  上で、上記(20)のように表される多項式の各係数と相互に独立に積がとられることに注意すると、上記(20)の多項

式の係数に対応する  $F_q$  上のベクトル  $(c_{i1}^{(j)}, c_{i2}^{(j)}, \dots, c_{iK}^{(j)})$  は、受信者のみが知る順序で適切に、しかし各クラス同一の置換によって、ランダムにスクランブルすることができる。従って、この置換行列  $P(*)$  を秘密鍵として設計者は保存することができる。このことにより、公開情報に対する数論的攻撃は、 $K \geq 30$  程度になると現実的に不可能となる。例えば、 $F_q$  の  $q = 2^k$  の  $k = 16$  として  $K = 32$  とした場合に、正しい順序を求めるために必要な総当たりの回数は近似的に  $2.6 \times 10^{35}$  で与えられる。

【0065】

暗号文  $C$  のベクトル表現を、下記 (21) とする。但し、その各成分は下記 (22) のように設定する。

$$C = (C_1, C_2, \dots, C_K) \quad \dots (21)$$

【0066】

【数14】

$$C_i = \sum_{t=1}^K m_i c_{it}^{(1)} \quad \dots (22)$$

【0067】

ここで  $C_i, m_i, c_{ii}^{(j)} \in F_q$  であることに着目すると、上記 (22) に対してLLL法による攻撃を適用することは困難である。但し、上記 (22) は単純な線形変換によって解読されてしまうことは自明であるので、 $J \geq 2$  とすることが必須である。一方、公開鍵のランダムな選択は  $J^{K-1}$  通り (第1例)、 $J^{K-2}$  通り (第2例) 存在し、 $J^{K-1} \gg 1, J^{K-2} \gg 1$  とすることが可能である。よって、この第2実施の形態の公開鍵暗号に対する攻撃は逐一的にしか行うことができず、この暗号化・復号手法は極めて強力である。

【0068】

なお、第1実施の形態における公開鍵サイズ、各エンティティの暗号化用鍵サイズは以下のように与えられる。

公開鍵サイズ:  $J K^2$  kビット

エンティティの暗号化用鍵サイズ： $K^2$  kビット

【0069】

ここで、暗号通信開始時には、メッセージが符号化されているので、上記（9），（18）の条件より下記（23）の条件が満たされねばならず、レート（情報伝送率）は1未満となる。

$$J < 2^k \quad \dots (23)$$

しかしながら、ある一定期間または一定量のデータを送っている間は選択鍵が固定されているような場合には、上記（23）の条件は外され、レートはほぼ1となる。

【0070】

具体的な数値例について説明する。

〈数値例1〉

比較的大きな例として  $k=16$ ， $K=1024$ ， $J=1024$  とした場合に、公開鍵サイズは  $2^{10} \cdot 2^{20} \cdot 2^4 = 2^{34}$  ビット  $\approx 2.147$  ギガバイト、エンティティの暗号化用鍵サイズは2.0 キロバイトとなる。

【0071】

〈数値例2〉

比較的小さな例として  $k=8$ ， $K=128$ ， $J=128$  とした場合に、公開鍵サイズは2.097 メガバイト、エンティティの暗号化用鍵サイズは16.384キロバイトとなる。

【0072】

〈数値例3〉

$k=16$ ， $K=128$ ， $J=128$  とした場合に、公開鍵サイズは4.19メガバイト、エンティティの暗号化用鍵サイズは32.8キロバイトとなり、暗号化のための主要な演算： $F_q$ （ $q=2^{16}$ ）の元128個の積和演算（128重の平行処理により7ステップで実行）となり、復号のための主要な演算： $F_q$ （ $q=2^{16}$ ）上の128次の多項式による乗除算1回及び  $F_q$ （ $q=2^{16}$ ）上の1次の多項式による逐次的な乗除算128回となる。

【0073】

## 〈数値例 4〉

$k = 8$ ,  $K = 32$ ,  $J = 16$ とした場合に、公開鍵サイズは16.4キロバイト、エンティティの暗号化用鍵サイズは1.02キロバイトとなり、暗号化のための主要な演算： $F_q$  ( $q = 2^8$ ) の元32個の積和演算 (32重の平行処理により5ステップで実行) となり、復号のための主要な演算： $F_q$  ( $q = 2^8$ ) 上の32次の多項式による乗除算1回及び  $F_q$  ( $q = 2^8$ ) 上の1次の多項式による逐次的な乗除算32回となる。

## 【0074】

以下、第2例におけるレートとその改善とについて説明する。秘密の多項式  $P(X)$  の次数は  $K + 1$  であるので、入力平文長  $L_M$ , 出力暗号文長  $L_C$  は夫々下記 (24), (25) で与えられ、レート  $r$  は下記 (26) のようになる。

$$L_M = K k \quad \dots (24)$$

$$L_C = (K + 1) k \quad \dots (25)$$

$$r = K / (K + 1) \quad \dots (26)$$

## 【0075】

ここで、レート  $r$  を完全に1にすることを考える。クラス1における基数  $b_1^{(j)}$  を全て定数項のみとする。即ち、 $b_1^{(j)} = \alpha_1^{(j)}$  とする。この場合、下記 (27) を満たすとし、係数ベクトル  $(w_1^{(j)}, w_2^{(j)}, \dots, w_K^{(j)})$  の成分をランダムに置換したベクトル  $P(w_1^{(j)}, w_2^{(j)}, \dots, w_K^{(j)})$  を導き、これらを公開鍵リストのクラス1のサブ鍵とする。

## 【0076】

## 【数15】

$$\begin{aligned} \alpha_1^{(j)} w(X) = & w_1^{(j)} + w_2^{(j)} X + w_3^{(j)} X^2 + \dots \\ & + w_K^{(j)} X^{K-1} \dots (27) \end{aligned}$$

## 【0077】

このようにしても  $K \gg 1$  であれば、 $P(w_1^{(j)}, w_2^{(j)}, \dots, w_K^{(j)})$

に対する総当たりの攻撃は、依然として現実的に不可能である。

#### 【0078】

以上により、入力平文長  $L_M$ ，出力暗号文長  $L_C$ ，レート  $r$  は、夫々下記 (28)，(29)，(30) で与えられることがわかる。

$$L_M = K k \quad \dots (28)$$

$$L_C = K k \quad \dots (29)$$

$$r = 1 \quad \dots (30)$$

#### 【0079】

(第2実施の形態：有限体上での誤り訂正符号を利用した積和型暗号)

図4は、第2実施の形態による暗号化方法・復号方法をエンティティ a，b 間の情報通信に利用した状態を示す模式図である。図1と同様に、図4の例でも、一方のエンティティ a 側で、平文 M を暗号文 C に暗号化し、通信路 1 を介してその暗号文 C を他方のエンティティ b へ送信し、エンティティ b 側で、その暗号文 C を元の平文 M に復号する。

#### 【0080】

送信側であるエンティティ a には、平文 M を複数の分割平文に分割する平文分割器 2 と、公開鍵と各分割平文とを用いて暗号文 C を作成する暗号化器 3 とが備えられている。また、受信側であるエンティティ b には、送られてきた暗号文 C を元の平文 M に復号する復号器 4 が備えられている。第2実施の形態では、第1実施の形態と同様に、秘密鍵，公開鍵，乱数等を多項式表現して、有限体上で積和型暗号系を構成する。

#### 【0081】

(暗号化)

秘密鍵と公開鍵とを以下のように準備する。

- ・秘密鍵： $\{X^a g_i(X)\}$ ， $w(X)$ ， $P(X)$
- ・公開鍵： $\{C_i(X)\}$   $m$  に対する符号化パラメータ

#### 【0082】

次数  $g_i$  の  $F_2$  上の符号多項式を  $g_i(X)$  とする。但し、ここでは説明を簡単にするために、 $g_i = g$  (一定) とする。  $P(X)$  を適切に選ばれた秘密の多

項式として、下記 (31) を導く。なお、上記  $g_i$  と同様に、 $a_i = a$  (一定) とする。

【0083】

【数16】

$$X^{a_i} g_i(X) w(X) \equiv C_i(X) \pmod{P(X)} \quad \dots (31)$$

【0084】

暗号化を、下記 (32) のように行う。

【0085】

【数17】

$$C(X) = \sum_{i=1}^K m_i'(X) C_i(X) \quad \dots (32)$$

【0086】

(復号)

〔第2実施の形態の第1復号例〕

下記 (33) を満たす秘密の多項式  $w^{-1}(X)$  を用いて、中間復号文  $M(X)$  を下記 (34) のように導く。この中間復号文  $M(X)$  は、具体的には下記 (35) のように求められる。

$$w(X) w^{-1}(X) \equiv 1 \pmod{P(X)} \quad \dots (33)$$

$$M(X) \equiv C(X) w^{-1}(X) \pmod{P(X)} \quad \dots (34)$$

【0087】

【数18】

$$\begin{aligned} M(X) = & g_1(X) m_1'(X) + g_2(X) m_2'(X) X^a \\ & + \dots + g_K(X) m_K'(X) X^{(K-1)a} \quad \dots (35) \end{aligned}$$

【0088】

以上において、秘密の多項式  $P(X)$  の次数  $p$  を、上記 (35) の右辺の次数より 1 だけ高い値に設定しておく。即ち、 $p$  は下記 (36) の条件を満たす。

$$p = g + k + (K - 1) a + 1 \quad \dots (36)$$

【0089】

ベクトル  $w$  の下位  $n$  桁をサンプルする操作を  $S_a(w)$  と表記し、サンプルされた系列を多項式では  $S_w(X)$  と記す。ここで、以下 (a), (b) のことが成立する。

【0090】

(a) : 上記 (35) で与えられる中間復号文  $M(X)$  に対してサンプルされた系列  $S_w(X)$  において、 $a < g + k = n$  となる場合に、第 2 項の長さ  $(g + k - a)$  の末端  $e_1(X)$  が、下記 (37) のように、加算された形になっている。

$$g_1(X) m_1(X) + e_1(X) X^a \quad \dots (37)$$

(b) : 末端  $e_1(X)$  の次数を  $(e - 1)$  とした場合、 $g \geq e$  となるときに、 $e_1(X)$  は消失誤りとして訂正可能である。

【0091】

この (a), (b) によって、 $S_w(X)$  における  $e_1(X) X^a$  を消失誤りとして訂正でき、 $g_1(X) m_1(X)$  を復号して、これより容易に  $m_1(X)$  を復号できる。つまり、上記 (37) のように、中間復号文の各項では、積和成分にノイズ成分が加算された形になっているが、その積和成分が誤り訂正符号語になっているので、その誤り訂正能力によってノイズ成分を誤りとして訂正することができ、正しく積和成分のみを復号できる。なお、第 2 項以降も、第 1 項と同様に復号することができる。以上のように、第 1 復号例では、最下位項から上位項側に順次的に復号している。

【0092】

〔第 2 実施の形態の第 2 復号例〕

下記 (38) を満たす秘密の多項式  $w^{-1}(X)$  を用いて、中間復号文  $M(X)$  を下記 (39) のように導く。この中間復号文  $M(X)$  は、具体的には下記 (40) のように求められる。

$$w(X) w^{-1}(X) \equiv 1 \pmod{P(X)} \quad \dots (38)$$

$$M(X) \equiv C(X) w^{-1}(X) \pmod{P(X)} \quad \dots (39)$$

【0093】

【数19】

$$M(X) = g_1(X)m_1'(X) + g_2(X)m_2'(X)X^a \\ + \dots + g_K(X)m_K'(X)X^{(K-1)a} \quad \dots (40)$$

【0094】

ここで、以下(c)，(d)のことが成立する。

(c)：上記(40)で与えられる中間復号文 $M(X)$ に対してサンプルされた系列 $S_w(X)$ において、 $a < g + k = n$ となる場合に、第2項 $g_{K-1}(X)m_{K-1}'(X)$ の上位 $(g + k - a)$ 桁の $e_{K-1}(X)$ が、下記(41)のように、加算された形になっている。

$$g_K(X)m_K'(X) + e_{K-1}(X)X^a \quad \dots (41)$$

(d)： $e_{K-1}(X)$ の次数を $(e-1)$ とした場合、 $g \geq e$ となるときに、 $e_{K-1}(X)$ は消失誤りとして訂正可能である。

【0095】

この(c)，(d)によって、 $S_w(X)$ における $e_{K-1}(X)$ を消失誤りとして訂正し、 $g_K(X)m_K'(X)$ を復号して、これより容易に $m_K'(X)$ を復号できる。以上のように、第2復号例では、最上位項から下位項側に順次的に復号している。

【0096】

ところで、この第2実施の形態においても、上述した第1実施の形態のように、公開鍵を任意に選択するような方式が可能である。即ち、第1実施の形態の第1例に適用する場合、 $g_i(X)$ はクラス $i$ に属するとし、クラス1以外のクラスにあっては各 $J$ 個の $g_i(X)$ を準備しておき、クラス1において復号された $m_1(X)$ より $m_1$ を復号し、全く同様にして、クラス2における公開鍵の選択情報を得ることができる。また、第1実施の形態の第2例に適用する場合、 $g_i(X)$ はクラス $i$ に属するとし、クラス $K$ ， $K-1$ 以外のクラスにあっては各 $J$



個の  $g_i(X)$  を準備しておき、クラス  $K$  において復号された  $m_K(X)$  より  $m_K$  を復号し、全く同様に、クラス  $K-2$  における公開鍵の選択情報を得ることができる。

【0097】

図5は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、上述した第1実施の形態または第2実施の形態における符号化処理または復号処理を含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ20は、各エンティティ側に設けられている。

【0098】

図5において、コンピュータ20とオンライン接続する記録媒体21は、コンピュータ20の設置場所から隔たって設置される例えばWWW(World Wide Web)のサーバコンピュータを用いてなり、記録媒体21には前述の如きプログラム21aが記録されている。記録媒体21から読み出されたプログラム21aがコンピュータ20を制御することにより、コンピュータ20が平文から暗号文を作成するか、または、暗号文を平文に復号する。

【0099】

コンピュータ20の内部に設けられた記録媒体22は、内蔵設置される例えばハードディスクドライブまたはROM等を用いてなり、記録媒体22には前述の如きプログラム22aが記録されている。記録媒体22から読み出されたプログラム22aがコンピュータ20を制御することにより、コンピュータ20が平文から暗号文を作成するか、または、暗号文を平文に復号する。

【0100】

コンピュータ20に設けられたディスクドライブ20aに装填して使用される記録媒体23は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスク等を用いてなり、記録媒体23には前述の如きプログラム23aが記録されている。記録媒体23から読み出されたプログラム23aがコンピュータ20を制御することにより、コンピュータ20が平文から暗号文を作成するか、または、暗号文を平文に復号する。

【0101】

【発明の効果】

以上のように、本発明では、有限体上で積和型暗号系を構成するようにしたので、整数環上での積和型暗号系に比べてLLL法による攻撃に対して強くなり、安全性を向上できる。

【0102】

また、中間復号文の各項が誤り訂正符号語で構成されるようにしたので、多少の誤りが発生しても、その符号語の訂正能力により元の平文を正確に復号できる。

【0103】

更に、平文を分割した分割平文毎に複数の公開鍵が予め準備しておき、準備されているそれらの複数の公開鍵から任意の公開鍵を各分割平文毎に選択し、選択した公開鍵を使用して暗号文を作成するようにしたので、自由に公開鍵を選択して暗号文を作成できて、その公開鍵の選択の仕方が攻撃者には不明であるため、攻撃は困難となり、安全性を更に向上することができる。

【0104】

(付記)

なお、以上の説明に対して更に以下の項を開示する。

(1) 請求項3記載の暗号化方法であって、所定数の分割平文に対する公開鍵は固定である暗号化方法。

(2) 請求項3記載の暗号化方法であって、ある分割平文に対して選択した公開鍵を示す選択情報を、その分割平文から所定数ずらせた他の分割平文に盛り込んで暗号文を作成する暗号化方法。

(3) 第(1)または(2)項記載の暗号化方法であって、前記所定数は1または2である暗号化方法。

(4) 請求項1～3及び第(1)～(3)項の何れかに記載の暗号化方法によって作成された積和型の暗号文を復号する復号方法であって、前記暗号文の最下位項の分割平文から始めて上位項側へ各分割平文を順次復号していく復号方法。

(5) 請求項1～3及び第(1)～(3)項の何れかに記載の暗号化方法によって作成された積和型の暗号文を復号する復号方法であって、前記暗号文の最上

位項の分割平文から始めて下位項側へ各分割平文を順次復号していく復号方法。

(6) 第(2)項記載の暗号化方法によって作成された積和型の暗号文を復号する復号方法であって、分割平文を復号する処理と、選択情報を復号する処理とを並列的に行う復号方法。

(7) 一方のエンティティ側で平文を分割した分割平文と公開鍵とを用いて積和型の暗号文を作成して他方のエンティティ側へ伝送し、伝送された暗号文を該他方のエンティティ側で平文に復号することにより、エンティティ間で情報の通信を行う暗号通信方法において、前記積和型の暗号文を有限体上で構成する暗号通信方法。

(8) 複数のエンティティ間で暗号文による情報通信を行う暗号通信システムにおいて、請求項1～3及び第(1)～(3)項の何れかに記載の暗号化方法を用いて平文から暗号文を作成する暗号化器と、作成した暗号文を一方のエンティティから他方のエンティティへ送信する通信路と、送信された暗号文から平文を復号する復号器とを備える暗号通信システム。

(9) コンピュータに、暗号化すべき平文を分割した分割平文と公開鍵とを用いて暗号文を作成させるためのプログラムが記録されているコンピュータでの読み取りが可能な記録媒体において、請求項1～3及び第(1)～(3)項の何れかに記載の暗号化方法に従って暗号文を作成することをコンピュータに実行させるプログラムコード手段を含むプログラムが記録されている記録媒体。

【図面の簡単な説明】

【図1】

第1実施の形態での2人のエンティティ間における情報の通信状態を示す模式図である。

【図2】

第1実施の形態の第1例におけるデータベース内の公開鍵リストを示す図である。

【図3】

第1実施の形態の第2例におけるデータベース内の公開鍵リストを示す図である。

【図 4】

第 2 実施の形態での 2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 5】

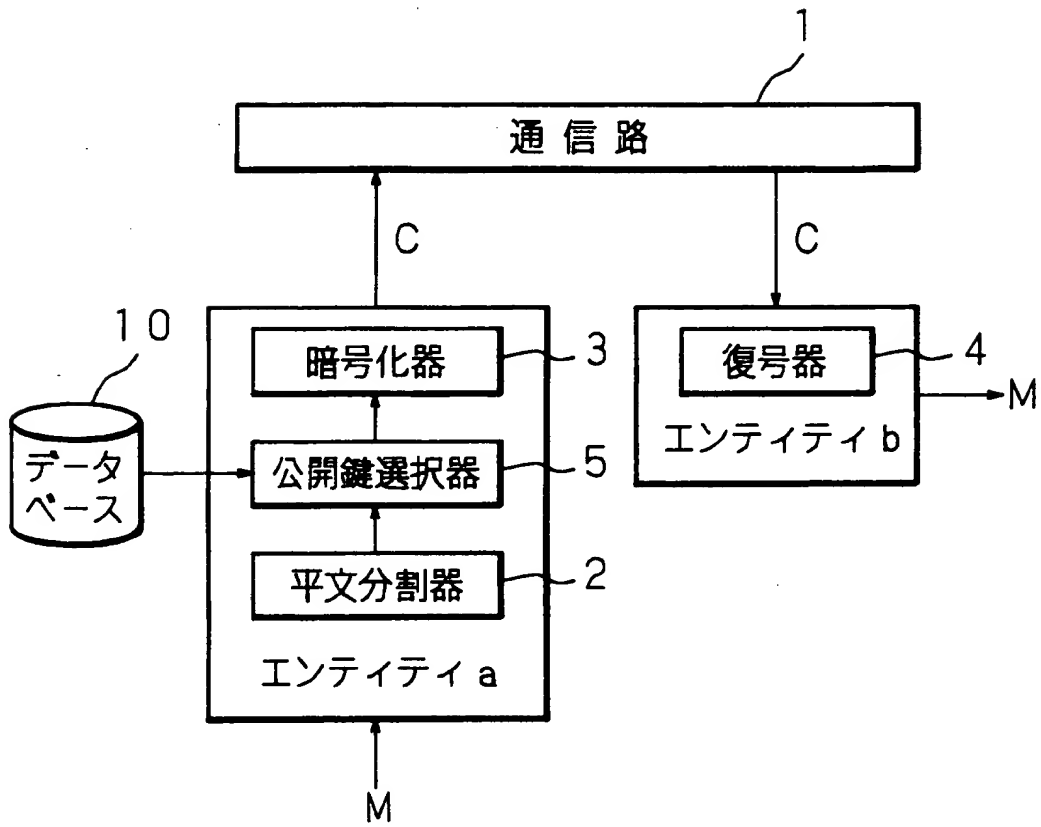
記録媒体の実施の形態の構成を示す図である。

【符号の説明】

- 1 通信路
- 2 平文分割器
- 3 暗号化器
- 4 復号器
- 5 公開鍵選択器
- 10 データベース
- 20 コンピュータ
- 21, 22, 23 記録媒体
- a, b エンティティ

【書類名】 図面

【図 1】



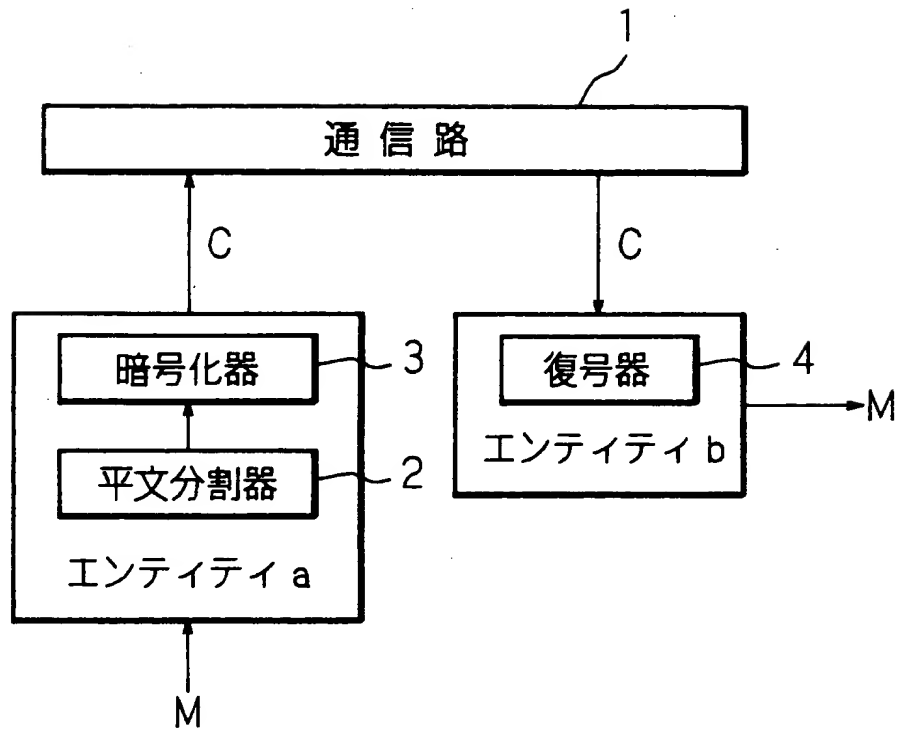
【図 2】

クラス1	クラス2	...	クラスK
$v_1(X)$	$b_1(X) v_2^{(1)}(X)$	...	$b_1(X) b_2(X) \cdots b_{K-1}(X) v_K^{(1)}(X)$
	$b_1(X) v_2^{(2)}(X)$	...	$b_1(X) b_2(X) \cdots b_{K-1}(X) v_K^{(2)}(X)$
	$\vdots$		$\vdots$
	$b_1(X) v_2^{(J)}(X)$	...	$b_1(X) b_2(X) \cdots b_{K-1}(X) v_K^{(J)}(X)$

【図3】

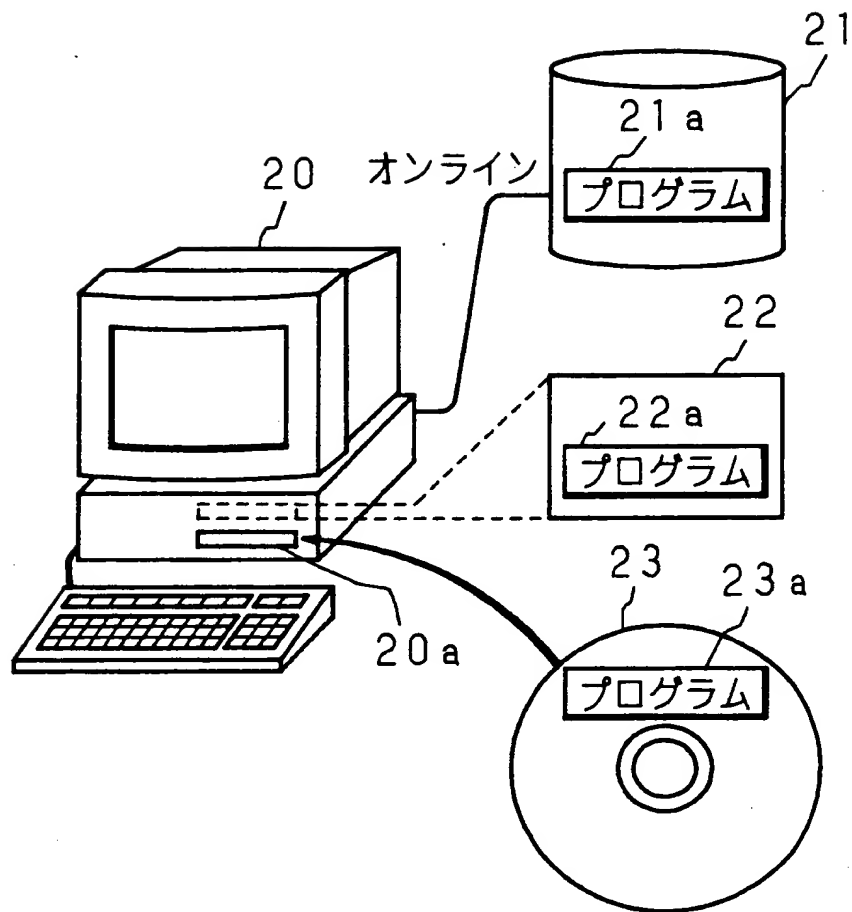
クラス 1	クラス 2	...	クラス K-2	クラス K-1	クラス K
$b_1^{(1)}$	$b_2^{(1)}X$	...	$b_{K-2}^{(1)}X^{K-3}$	$b_{K-1}X^{K-2}$	$b_KX^{K-1}$
$b_1^{(2)}$	$b_2^{(2)}X$	...	$b_{K-2}^{(2)}X^{K-3}$		
$\vdots$	$\vdots$		$\vdots$		
$b_1^{(j)}$	$b_2^{(j)}X$	...	$b_{K-2}^{(j)}X^{K-3}$		

【図 4】





【図5】



【書類名】 要約書

【要約】

【課題】 LLL法による攻撃に対して強く、安全性を向上できる新しい手法の積和型の暗号化方法を提供する。

【解決手段】 分割平文，秘密鍵，公開鍵，乱数等を多項式表現して、有限体上で積和型の暗号系を構成する。分割平文を符号化して、中間復号文の各項を誤り訂正符号語で構成する。各分割平文毎に任意の公開鍵を選択する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日	1990年 8月 7日
[変更理由]	新規登録
住 所	京都府京都市南区吉祥院南落合町3番地
氏 名	村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [597008636]

1. 変更年月日	1997年 1月21日
[変更理由]	新規登録
住 所	大阪府箕面市栗生外院4丁目15番3号
氏 名	笠原 正雄